インターネットを安全に使いましょう

広報委員　㈲西日本不動産　戸井　泰弘

情報化社会における今日では、インターネットは必要不可欠なものとなっています。そこで、インターネットの安全な使い方について（私のような初心者向けに）少しだけ調べてみました。最近のコンピュータウイルスは表面上パソコンには何も起こさず個人情報を抜き出して、犯罪目的（個人情報を売買したり、クレジットカードの不正使用等）に使ったりするといわれています。安全対策や最低限のルールやマナーを守り正しく使いましょう。

●最近は、パソコンでメールのやり取りをされる方も多いと思いますが、心当たりのない**添付ファイルがある迷惑メール**や、**フィッシング**「金融機関等の実在する企業を装い電子メールを送りつけ、その企業のウエブサイトに見せかけた偽のウエブサイトに誘導して、個人情報等を入力させ不正に入手することです」にじゅうぶん注意しましょう。金融機関等が、メールで口座番号や暗証番号等の重要な個人情報を問い合せることはないので、そうしたことを照会するメールは「フィッシング詐欺」と思って間違いないといわれています。また、知人から届いたメールでも不審に思われる添付ファイルが付いていたら、知人に送ったかどうか確認をしたり、ウイルスチェック等をしてから開きましょう。また、最近のメールソフトには、初期設定でプレビューウインドウやHTML表示が自動的に開くようになっているものがあるので、お使いのパソコン等の取扱説明書などを読み、自動的に開かないように設定変更をされるのも、ウイルスの感染、迷惑メール等の対策に効果があるのではないでしょうか。

●**ファーミング**「実在のURLを乗っ取り、多数の人を偽のホームページに誘い込み、大量の個人情報を収集する（詐欺の手口）」といわれています。ファーミングは、コンピュータウイルス等を使いパソコン内のファイルやサーバーの情報を書き換えることで、正しいURLを入力しても偽のホームページに誘導するように仕向けるので、URLが正しいから、個人情報を入力しても大丈夫と思っていると、ID・パスワード、クレジットカード番号等の個人情報を盗まれる可能性があるといわれています。**ファーミング対策**としては、インターネットに接続するのに必要なシステムファイルをウイルスやスパイウエアにより書き換えられない様、日頃からセキュリティ対策を忘れないようにし、こまめにWindows等を最新の状態にし、セキュリティ対策ソフトはたえずアップデートを行い、定期的にウイルスチェックを行いましょう。また、インターネットショッピング等をする際、パスワードやクレジットカード番号等の重要な個人情報を**入力するホームページ**に、SSLが使われているかどうか確認しましょう。SSLを使うには、そのホームページを運営する組織が、認証局と呼ばれる電子証明書の発行機関にドメイン名や会社の情報等を提出し審査を受け電子証明書を取得しなければならないので、証明書を取得してSSLを使っているホームページであれば、一応、安全といえるようです。但し、証明書を偽造して表示するホームページもあるので、証明書が表示されているからといっても油断は禁物でしょう。

●**スパイウエア**「ウイルスのようにパソコンに侵入して、タイピング、画面表示、ハードディスク等から個人情報等を盗み悪意のあるものに送信するプログラムです」を用いて盗んだ個人情報等を悪用して銀行口座等から預金を引き出す

等の犯罪が発生していると、マスコミ等で報じられた時期もありました。**スパイウエア対策**としては不審なCD－ROMやソフトウエアを使用しないこと、スパイウエア検出機能付きウイルス対策ソフトを使用する。また、ブラウザ（Internet Explorer等）のオートコンプリート「アドレス（URL）等の最初の数文字を入力しただけで、過去に入力した文字列が候補として表示される機能」が有効になっている場合には、お使いのパソコン等の取扱説明書などを見て、OFFにしておく等が挙げられています。

●**コンピュータウイルス**は、メール送信元のパソコンがウイルス等に感染していた場合に、送信元から届いたメールや添付ファイル等から感染したり、あるいはホームページを見た場合、ブラウザ（Internet Explorer等）の脆弱性「（**ぜいじゃくせい**）（一般的にコンピュータやネットワークにおけるセキュリティ上の弱点を意味し、第三者によるシステムへの侵入や攻撃（データの改ざん等）に利用される危険性がある）」を判別されたパソコンにウイルスを仕込まれる等で、一部のソフトウエアにはWindows　Update等やセキュリティ対策ソフトで補えない場合があるので、使っているソフトウエアのアップデートをしたり、定期的にアップデート情報を確認しましょう。

特に一般的なコンピュータウイルス

ファイル感染型（プログラムファイル等に感染し、ファイルを実行した場合に、問題を引き起こし、WordやExcel等のファイルに感染するウイルスをマクロウイルスといい、簡単に作成できるので無数のウイルスが日々発生し続けているといわれています。）

トロイの木馬型（一見、何でもないプログラムの中に、不正な動作を行う仕掛けを隠し持つウイルスをトロイの木馬といい、一般的に、ほかのファイルには感染せず、単独で不正な動作を行い、メールの添付ファイルを開いたり、インターネットからファイルをダウンロードして実行したりするとパソコンに感染するといわれています。）

ワーム型（ファイルに感染するウイルスとは異なり、単独で自己のコピーを作りだし、データの破壊等をするウイルスをワームといい、ホームページを見たり、メールを読んだりするだけで感染する場合があるといわれていて、インターネット等を介して瞬時に他のパソコンに感染するため、問題になっているといわれています。）

●パスワードは大切な情報です。パスワードを悪意のある第三者が入手した場合、本人になりすましインターネットに接続したり、メールを盗み読むことができるので、防衛策としてパスワードを定期的に変更するのも有効です。**パスワード設定**については、できれば長いパスワード**８文字以上**にし、英大文字、英小文字、数字や記号等を組み合わせ、名前、電話番号、誕生日等は使わないようにし、再利用はしないようにしましょう。

●最近テレビ等で、企業スパイにUSBメモリーを使用するとか、車内に置き忘れたパソコンを盗まれて情報を悪用された話を耳にします。パソコン、USB等の社外等への持ち出しには、情報流出等の危険性が伴うので、管理には充分注意しましょう。